AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: Mark Stoneman, AUSA 3/25/2021

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Black Android Samsung smartphone model SM-G970U with call number 405-923-5072 and Android identification number d5d8a9cb6a95683b.	))))	Case No: M-21-196- S TE

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Charles Thumann, Federal Bureau of Investigation, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

CHARLES W. THUMANN
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: Mar 30, 2021

Judge's signature

City and State: Lawton, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge
Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Charles W. Thumann, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been a Special Agent (SA) of the FBI since July 2004. I have received specific training and experience in numerous methods of investigation, including, but not limited to, electronic and visual surveillance, general questioning of witnesses, the use of search warrants, the use of confidential sources/informants, the use of pen registers, and the use of undercover agents. Based on my training and experience relating to the investigation of child pornography, and based upon interviews I have conducted with other officers, defendants, informants, and other witnesses and participants in child exploitation, I am familiar with the ways that child pornography is manufactured and distributed. My familiarity includes the various means and methods by which producers of child pornography manufacture and distribute pornography, including their use of cellular smartphones.

2. As an SA, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and review of documents and records. This affidavit is made in

support of an application for a warrant to search the Samsung MS-G970U model smartphone with CALL NUMBER 405-923-5072 (hereinafter referred to as "the SUBJECT PHONE") belonging to James Scott TIGER (TIGER). The SUBJECT PHONE is currently located in the Western District of Oklahoma at the Absentee Shawnee Tribal Police Department (ASTPD) at 2025 S. Gordon Cooper Drive, Shawnee, Oklahoma. The SUBJECT PHONE is described in detail in Attachment A to this affidavit. I request a warrant to search the SUBJECT PHONE for the items specified in Attachment B hereto, which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of material containing child pornography and accessing material with the intent to view child pornography).

4. This investigation, described more fully below, has revealed that an individual knowingly utilized and accessed the SUBJECT PHONE to violate the foregoing statute, and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located on the SUBJECT PHONE.

5. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

BACKGROUND OF INVESTIGATION

6. On December 12, 2020, the FBI Oklahoma City Division, Norman Resident Agency received a telephone call from Absentee Shawnee Tribal Police Department (ASTPD)

Captain Jason Brinker regarding an allegation that TIGER had committed a crime unrelated to this search warrant application, which alleged crime occurred within Indian country in Norman, Oklahoma.

7. On December 12, 2020, FBI and ASTPD interviewed TIGER's mother regarding the unrelated allegations against TIGER.

8. On December 12, 2020, ASTPD arrested TIGER on tribal charges arising from the unrelated allegations. During his arrest, TIGER had two cell phones in his possession, which he asked to leave at his home in his mother's custody. ASTPD allowed TIGER to leave his cell phones with his mother. One of those phones was the SUBJECT PHONE.

9. Following TIGER's arrest, ASTPD interviewed TIGER's sister who informed them that he had texted her while he was hiding from police when police responded to the unrelated allegations. She also told ASTPD that TIGER had told her he had previously committed acts similar to those alleged from the December 12, 2020 investigation. She told ASTPD that TIGER had told her he had taken photos of the previous acts and stored them on his phone. Based on that information, ASTPD obtained a search warrant from the Tribal Court of the Absentee Shawnee Tribe of Oklahoma to seize the SUBJECT PHONE from TIGER's home. ASTPD seized the SUBJECT PHONE from TIGER's home and still have it in custody in their office located at 2025 S. Gordon Cooper Drive, Shawnee, Oklahoma, within the Western District of Oklahoma.

10. On January 4, 2021, TIGER's mother contacted the FBI to expressed concern about a handwritten letter she received from TIGER who was incarcerated at the Pottawatomie

County Public Safety Center in Shawnee, Oklahoma. TIGER's mother gave the handwritten letter to FBI. It reads as follows:

> The last thing I want to write about is my phone, in case this is the last time I can write or talk to you. I got awoken in my cell and taken out. I didn't even put on my glasses, but I was took into booking and seen the tribal cop. He handed me a paper showing a search warrant for some of my electronics. He asked for the password to my Samsung, he said they could send it off to FBI headquarters and get all the data off either way, so I gave him the password even though I knew what was on it. That was on the 15th[.] I'm not sure if they told you or by the time you get this if they tell you, but as of today they haven't came back and talked to me. I don't know what's wrong with me and why I liked them but I had a bunch, like a lot of pictures of boys. 12 and 13 some older, some younger all downloaded from a website. I have been disgusted with myself. I would have rather died before someone found that out about me. So after I gave them the code I knew my life was over. I went back to my cell and looked for ways to end it, there was none. Also I thought I couldn't do that to you without an explanation. I know this doesn't make it any better but I promise mom, it was purely art for me, I looked and admired but I would have never ever touched one. I always steered clear, and IF I was around a boy I was never alone. I'm sorry your son is a monster. I love you so much, and please get S[*redacted*][1] to do that quickly so I can write again. If you can write me, don't say anything about the boys, they take a pic of the letter and put it on the kiosk is how we get letters back.

TERMS

11. Based on my training and experience, I use the following technical terms and definitions:

a. "Computer," as used broadly herein, refers to "an electronic, magnetic, optical,

1 TIGER's sister.

electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones. *See* 18 U.S.C. § 1030(e)(1).

b. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

c. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

d. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178).

e. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

f. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

g. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

h. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT, RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

12. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from

contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view and/or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or

electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

13. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON DIGITAL MEDIA STORAGE DEVICES AND CHILD PORNOGRAPHY

14. The ability of a smartphone to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media used in smartphones has grown tremendously within the last several years. These storage devices can store thousands of images at very high resolution. Given the storage capabilities, modern cellular phones can retain many years' worth of a user's data, stored indefinitely. Even deleted data can often be forensically recovered.

15. As is the case with most digital technology, communications by way of smartphone can be saved on the device. Storing this information can be intentional, i.e., by saving an email as a file on the smartphone or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Further, even if deleted, forensic examination can sometimes recover files and data including deleted picture files. I know that smartphones can be forensically examined, and forensic analysts can learn much detail about the user's habits and online activities, including websites visited, files downloaded, Google searches performed, locations where the device was used, dominion and control information, etc.

16. Smartphones can store the equivalent of thousands of pages of digital information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires the searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks depending on the volume of the data stored, and it would be generally impossible to accomplish this kind of data search on site.

SPECIFICS OF SEARCH AND SEIZURE OF CELL PHONES

17. Searches and seizures of evidence from smartphones commonly require agents to download or copy information from the smartphones and its components, such as a flash drive or other digital storage units attached to the phone, to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true for the following two reasons:

a. Smartphone devices (like hard disks, diskettes, tapes, laser disks, magneto-opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all of the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching smartphones for criminal evidence is a highly technical process requiring

expert skill and a properly controlled environment. The vast array of smartphone hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a smartphone system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since smartphone evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

18. In order to fully retrieve data from a smartphone system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child exploitation where the evidence frequently includes graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all of the system software (operating systems or interfaces, and hardware drivers) and any application software which may have been used to create the data (whether stored on hard drives or on external media).

19. Furthermore, because there is probable cause to believe that the smartphone and its storage devices are all instrumentalities of crimes they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

20. The search procedure for electronic data contained in smartphone hardware, smartphone software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of smartphone systems to determine what, if any, storage devices or digital storage units have been connected to such smartphone systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such smartphone hardware, smartphone software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise

unlawfully possessed, or (5) evidence of the offense specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

SMARTPHONES

21. Finally, based on my training and experience, I know that people who use their smartphone to view/access/possess child pornography do so in private to avoid detection. I believe there is probable cause that the SUBJECT PHONE and other digital file storage device(s) attached to the SUBJECT PHONE will contain evidence of the aforementioned criminal violations, as set forth in detain in Attachment B.

22. Because the SUBJECT PHONE is already in the custody of law enforcement, I request permission to execute the search at any time in the day or night.

CONCLUSION

23. Based on the above information, there is probable cause to believe that the foregoing laws have been violated, and that the following property, evidence, fruits, and instrumentalities of these offenses are located on the SUBJECT PHONE.

24. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the SUBJECT PHONE, described in Attachment A, authorizing the seizure of the items described in Attachment B to this affidavit.

Charles W. Thumann
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 30th day of March 2021.

SHON T. ERWIN
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF THE SUBJECT PHONE

Black Android Samsung smartphone model SM-G970U with call number 405-923-5072. The SUBJECT PHONE has the following Android identification number d5d8a9cb6a95683b.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Computer(s), as broadly defined in 18 U.S.C. § 1030(e) and all other digital file storage devices, including (but not limited to) desktop computers, smart phones, e-readers, tablets, thumb drives, SD cards, DVDs, compact discs, and external hard drives; all computer hardware, computer software; computer related devices and documentation; computer passwords and data security devices; videotapes; video recording devices; video recording players; and video display monitors that may be, or are used to visually depict child pornography or child erotica, display or access information pertaining to a sexual interest in child pornography, display or access information pertaining to sexual activity with children, or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

3. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

4. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

11. Any and all cameras, film, videotapes or other photographic equipment capable of storing images or videos of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

12. Any and all visual depictions of minors.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale,

trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to ownership or use of the SUBJECT PHONE.

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).